1

Introduction

In recent years automatic identification procedures (Auto-ID) have become very popular in many service industries, purchasing and distribution logistics, industry, manufacturing companies and material flow systems. Automatic identification procedures exist to provide information about people, animals, goods and products in transit.

The omnipresent barcode labels that triggered a revolution in identification systems some considerable time ago, are being found to be inadequate in an increasing number of cases. Barcodes may be extremely cheap, but their stumbling block is their low storage capacity and the fact that they cannot be reprogrammed.

The technically optimal solution would be the storage of data in a silicon chip. The most common form of electronic data-carrying devices in use in everyday life is the smart card based upon a contact field (telephone smart card, bank cards). However, the mechanical contact used in the smart card is often impractical. A contactless transfer of data between the data-carrying device and its reader is far more flexible. In the ideal case, the power required to operate the electronic data-carrying device would also be transferred from the reader using contactless technology. Because of the procedures used for the transfer of power and data, contactless ID systems are called *RFID systems* (radio frequency identification).

The number of companies actively involved in the development and sale of RFID systems indicates that this is a market that should be taken seriously. Whereas global sales of RFID systems were approximately 900 million $US in the year 2000 it is estimated that this figure will reach 2650 million $US in 2005 (Krebs, n.d.). The *RFID market* therefore belongs to the fastest growing sector of the radio technology industry, including mobile phones and cordless telephones (Figure 1.1).

Furthermore, in recent years contactless identification has been developing into an independent interdisciplinary field, which no longer fits into any of the conventional pigeonholes. It brings together elements from extremely varied fields: RF technology and EMC, semiconductor technology, data protection and cryptography, telecommunications, manufacturing technology and many related areas.

As an introduction, the following section gives a brief overview of different automatic ID systems that perform similar functions to RFID (Figure 1.2).

RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, Third Edition. Klaus Finkenzeller

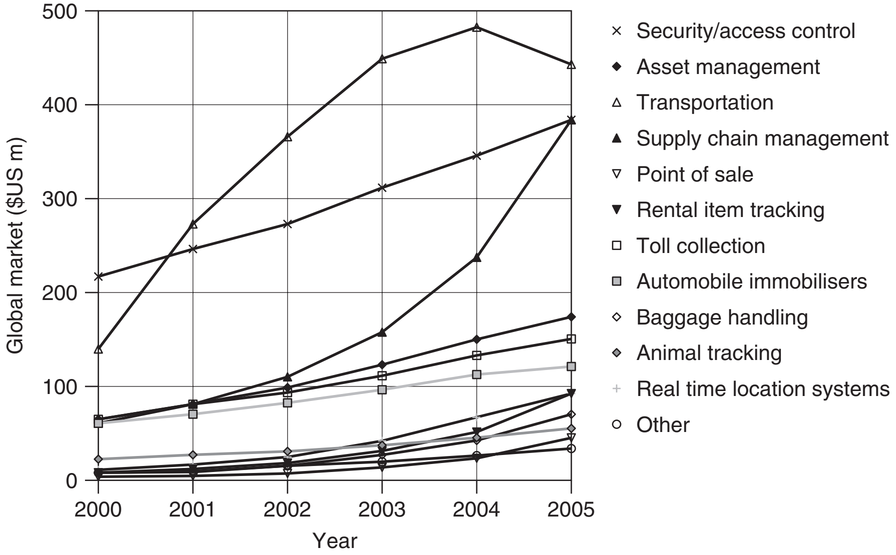


Figure 1.1 The estimated growth of the global market for RFID systems between 2000 and 2005 in million $US, classified by application (Krebs, n.d.)

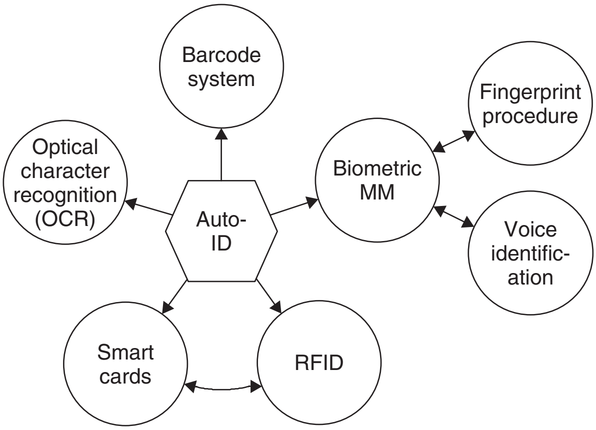
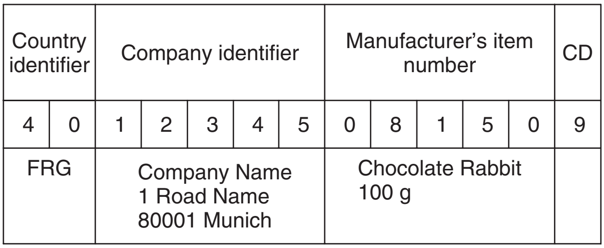


Figure 1.2 Overview of the most important auto-ID procedures

1.1 Automatic Identification Systems

1.1.1 Barcode Systems

Barcodes have successfully held their own against other identification systems over the past 20 years. According to experts, the turnover volume for barcode systems totalled around 3 billion DM in Western Europe at the beginning of the 1990s (Virnich and Posten, 1992).



Country identifier		Company identifier					Manufacturer's item number					CD
4	0	1	2	3	4	5	0	8	1	5	0	9
FRG		Company Name 1 Road Name 80001 Munich					Chocolate Rabbit 100 g					

Figure 1.3 Example of the structure of a barcode in EAN coding

Table 1.1 Common barcodes with typical applications

Code	Typical application
Code Codabar	Medical/clinical applications, fields with high safety requirements
Code 2/5 interleaved	Automotive industry, goods storage, pallets, shipping containers and heavy industry
Code 39	Processing industry, logistics, universities and libraries

The barcode is a binary code comprising a field of bars and gaps arranged in a parallel configuration. They are arranged according to a predetermined pattern and represent data elements that refer to an associated symbol. The sequence, made up of wide and narrow bars and gaps, can be interpreted numerically and alphanumerically. It is read by optical laser scanning, i.e. by the different reflection of a laser beam from the black bars and white gaps (ident, 1996). However, despite being identical in their physical design, there are considerable differences between the code layouts in the approximately ten different barcode types currently in use.

The most popular barcode by some margin is the *EAN code* (European Article Number), which was designed specifically to fulfil the requirements of the grocery industry in 1976. The EAN code represents a development of the UPC (Universal Product Code) from the USA, which was introduced in the USA as early as 1973. Today, the UPC represents a subset of the EAN code, and is therefore compatible with it (Virnich and Posten, 1992).

The EAN code is made up of 13 digits: the country identifier, the company identifier, the manufacturer's item number and a check digit.

In addition to the EAN code, the barcodes shown in Table 1.1 are popular in other industrial fields.

1.1.2 Optical Character Recognition

Optical character recognition (OCR) was first used in the 1960s. Special fonts were developed for this application that stylised characters so that they could be read both in the normal way by people and automatically by machines. The most important advantage of OCR systems is the high density of information and the possibility of reading data visually in an emergency, or simply for checking (Virnich and Posten, 1992). Today, OCR is used in production, service and administrative fields, and also in banks for the registration of cheques (personal data, such as name and account number, is printed on the bottom line of a cheque in OCR type). However, OCR systems have failed to become universally applicable because of their high price and the complicated readers that they require in comparison with other ID procedures.

1.1.3 Biometric Procedures

Biometrics is defined as the science of counting and (body) measurement procedures involving living beings. In the context of identification systems, biometry is the general term for all procedures that identify people by comparing unmistakable and individual physical characteristics. In practice, these are fingerprinting and handprinting procedures, voice identification and, less commonly, retina (or iris) identification.

1.1.3.1 Voice Identification

Recently, specialised systems have become available to identify individuals using speaker verification (speaker recognition). In such systems, the user talks into a microphone linked to a computer. This equipment converts the spoken words into digital signals, which are evaluated by the identification software.

The objective of speaker verification is to check the supposed identity of the person based upon their voice. This is achieved by checking the speech characteristics of the speaker against an existing reference pattern. If they correspond, then a reaction can be initiated (e.g. ‘open door’).

1.1.3.2 Fingerprinting Procedures (Dactyloscopy)

Criminology has been using fingerprinting procedures for the identification of criminals since the early twentieth century. This process is based upon the comparison of papillae and dermal ridges of the fingertips, which can be obtained not only from the finger itself, but also from objects that the individual in question has touched.

When fingerprinting procedures are used for personal identification, usually for entrance procedures, the fingertip is placed upon a special reader. The system calculates a data record from the pattern it has read and compares this with a stored reference pattern. Modern fingerprint ID systems require less than half a second to recognise and check a fingerprint. In order to prevent violent frauds, fingerprint ID systems have even been developed that can detect whether the finger placed on the reader is that of a living person (Schmidhäusler, 1995).

1.1.4 Smart Cards

A *smart card* is an electronic data storage system, possibly with additional computing capacity (microprocessor card), which – for convenience – is incorporated into a plastic card the size of a credit card. The first smart cards in the form of prepaid telephone smart cards were launched in 1984. Smart cards are placed in a reader, which makes a galvanic connection to the contact surfaces of the smart card using contact springs. The smart card is supplied with energy and a clock pulse from the reader via the contact surfaces. Data transfer between the reader and the card takes place using a bidirectional serial interface (I/O port). It is possible to differentiate between two basic types of smart card based upon their internal functionality: the memory card and the microprocessor card.

One of the primary advantages of the smart card is the fact that the data stored on it can be protected against undesired (read) access and manipulation. Smart cards make all services that relate to information or financial transactions simpler, safer and cheaper. For this reason, 200 million smart cards were issued worldwide in 1992. In 1995 this figure had risen to 600 million, of which 500 million were memory cards and 100 million were microprocessor cards. The *smart card market* therefore represents one of the fastest growing subsectors of the microelectronics industry.

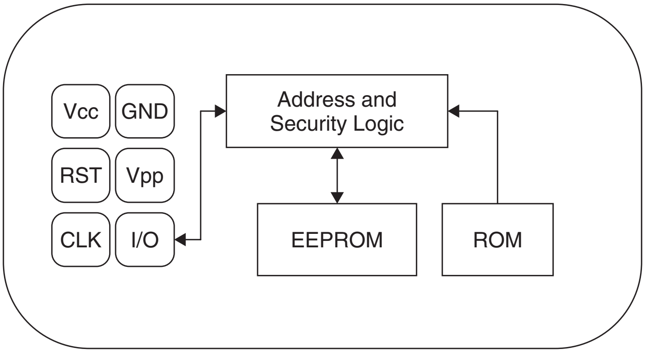


Figure 1.4 Typical architecture of a memory card with security logic

One disadvantage of contact-based smart cards is the vulnerability of the contacts to wear, corrosion and dirt. Readers that are used frequently are expensive to maintain due to their tendency to malfunction. In addition, readers that are accessible to the public (telephone boxes) cannot be protected against vandalism.

1.1.4.1 Memory Cards

In *memory cards* the memory – usually an EEPROM – is accessed using a sequential logic (state machine) (Figure 1.5). It is also possible to incorporate simple security algorithms, e.g. stream ciphering, using this system. The functionality of the memory card in question is usually optimised for a specific application. Flexibility of application is highly limited but, on the positive side, memory cards are very cost effective. For this reason, memory cards are predominantly used in price-sensitive, large-scale applications (Rankl and Effing, 1996). One example of this is the national insurance card used by the state pension system in Germany (Lemme, 1993).

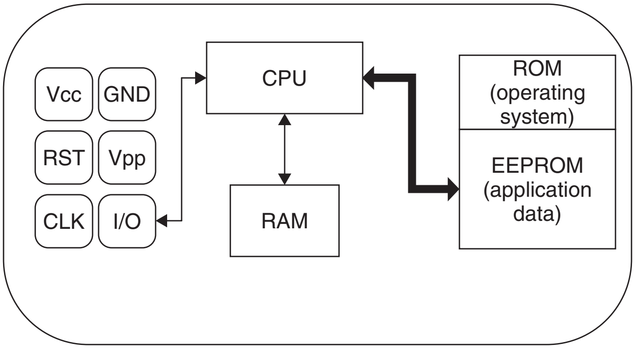


Figure 1.5 Typical architecture of a microprocessor card

1.1.4.2 Microprocessor Cards

As the name suggests, *microprocessor cards* contain a microprocessor, which is connected to a segmented memory (ROM, RAM and EEPROM segments).

The mask programmed ROM incorporates an *operating system* (higher program code) for the microprocessor and is inserted during chip manufacture. The contents of the ROM are determined during manufacturing, are identical for all microchips from the same production batch, and cannot be overwritten.

The chip's EEPROM contains application data and application-related program code. Reading from or writing to this memory area is controlled by the operating system.

The RAM is the microprocessor's temporary working memory. Data stored in the RAM are lost when the supply voltage is disconnected.

Microprocessor cards are very flexible. In modern smart card systems it is also possible to integrate different applications in a single card (multi-application). The application-specific parts of the program are not loaded into the EEPROM until after manufacture and can be initiated via the operating system.

Microprocessor cards are primarily used in security-sensitive applications. Examples are smart cards for GSM mobile phones and the new EC (electronic cash) cards. The option of programming the microprocessor cards also facilitates rapid adaptation to new applications (Rankl and Effing, 1996).

1.1.5 RFID Systems

RFID systems are closely related to the smart cards described above. Like smart card systems, data is stored on an electronic data-carrying device – the transponder. However, unlike the smart card, the power supply to the data-carrying device and the data exchange between the data-carrying device and the reader are achieved without the use of galvanic contacts, using instead magnetic or electromagnetic fields. The underlying technical procedure is drawn from the fields of radio and radar engineering. The abbreviation RFID stands for radio frequency identification, i.e. information carried by radio waves.

Due to the numerous advantages of RFID systems compared with other identification systems, RFID systems are now beginning to conquer new mass markets. One example is the use of contactless smart cards as tickets for short-distance public transport.

1.2 A Comparison of Different ID Systems

A comparison between the identification systems described above highlights the strengths and weakness of RFID in relation to other systems (Table 1.2). Here too, there is a close relationship between contact-based smart cards and RFID systems; however, the latter circumvent all the disadvantages related to faulty contacting (sabotage, dirt, unidirectional insertion, time-consuming insertion, etc.).

1.3 Components of an RFID System

An *RFID system* is always made up of two components (Figure 1.6):

- the *transponder*, which is located on the object to be identified;
- the interrogator or *reader*, which, depending upon the design and the technology used, may be a read or write/read device (in this book – in accordance with normal colloquial usage – the data capture device is always referred to as the *reader*, regardless of whether it can only read data or is also capable of writing).

Table 1.2 Comparison of different RFID systems showing their advantages and disadvantages

System parameters	Barcode	OCR	Voice recognition	Biometry	Smart card	RFID systems
Typical data quantity (bytes)	1–100	1–100	–	–	16–64 k	16–64 k
Data density	Low	Low	High	High	Very high	Very high
Machine readability	Good	Good	Expensive	Expensive	Good	Good
Readability by people	Limited	Simple	Simple	Difficult	Impossible	Impossible
Influence of dirt/damp	Very high	Very high	–	–	Possible (contacts)	No influence
Influence of (optical) covering	Total failure	Total failure	–	Possible	–	No influence
Influence of direction and position	Low	Low	–	–	Unidirectional	No influence
Degradation/wear	Limited	Limited	–	–	Contacts	No influence
Purchase cost/reading electronics	Very low	Medium	Very high	Very high	Low	Medium
Operating costs (e.g. printer)	Low	Low	None	None	Medium (contacts)	None
Unauthorised copying/modification	Slight	Slight	Possible* (audio tape)	Impossible	Impossible	Impossible
Reading speed (including handling of data carrier)	Low ~4 s	Low ~3 s	Very low >5 s	Very low >5–10 s	Low ~4 s	Very fast ~0.5 s
Maximum distance between data carrier and reader	0–50 cm	<1 cm Scanner	0–50 cm	Direct contact**	Direct contact	0–5 m, microwave

*The danger of ‘replay’ can be reduced by selecting the text to be spoken using a random generator, because the text that must be spoken is not known in advance.
**This only applies for fingerprint ID. In the case of retina or iris evaluation direct contact is not necessary or possible.

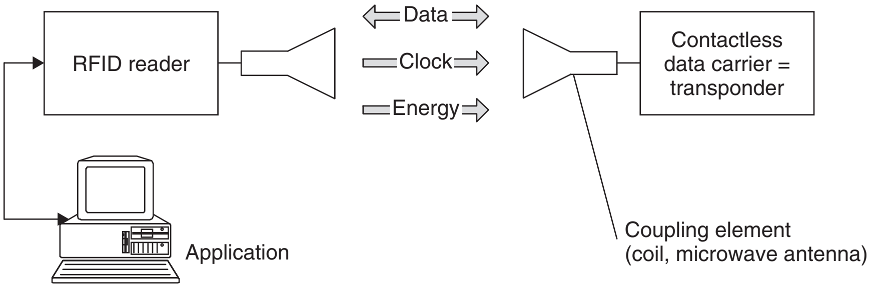

Data
Clock
Energy
RFID reader
Contactless data carrier = transponder
Application
Coupling element (coil, microwave antenna)

Figure 1.6 The reader and transponder are the main components of every RFID system

Figure 1.7 RFID reader and contactless smart card in practical use (reproduced by permission of Kaba Benzing GmbH)

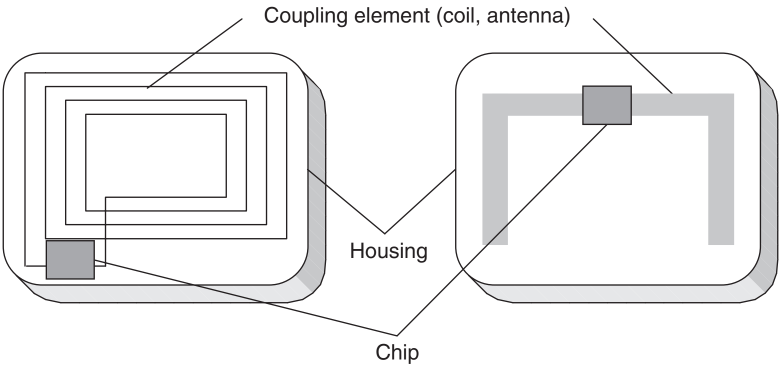


Figure 1.8 Basic layout of the RFID data-carrying device, the transponder. Left, inductively coupled transponder with antenna coil; right, microwave transponder with dipolar antenna

A reader typically contains a radio frequency module (transmitter and receiver), a control unit and a coupling element to the transponder. In addition, many readers are fitted with an additional interface (RS 232, RS 485, etc.) to enable them to forward the data received to another system (PC, robot control system, etc.).

The transponder, which represents the actual *data-carrying device* of an RFID system, normally consists of a *coupling element* and an electronic *microchip*. When the transponder, which does not usually possess its own voltage supply (battery), is not within the interrogation zone of a reader it is totally passive. The transponder is only activated when it is within the interrogation zone of a reader. The power required to activate the transponder is supplied to the transponder through the coupling unit (contactless), as are the timing pulse and data.